

REMARKS

The examiner rejected claims 1 and 3-9 under 35 U.S.C. §103 over U.S. Patent No. 5,878,231 to Baehr et al. in view of U.S. Patent No. 6,950,946 to Droz et al. The examiner stated that Baehr teaches essentially all of the features of the invention, but “fails to explicitly disclose the feature wherein the network interfaces...” do not “send physical addresses to the computer network”. The examiner stated that Droz teaches a physical address (MAC) that is hidden within a file or hard disk partition stored within the computer and cited column 7, lines 60-64 as support.

Applicant respectfully disagrees that Droz teaches the feature for which it was cited. Furthermore, even if Droz teaches this feature, this feature is not the limitation Applicant claims, as discussed in detail below.

Applicant’s screen “does not send physical addresses to the computer network” (see claim 1 and paragraph [0009] of “Clean Copy Of Substitute Specification”). Because of this feature, Applicant’s screen cannot be located by any tools of secured or open segments of the network. If Applicant’s screen cannot be located by a tool, it is not possible to disable or otherwise affect the screen. This makes Applicant’s screen remarkably effective at avoiding disablement.

The Droz reference is for locating/identifying a stolen computer that is later connected to a network, such as the Internet. Droz teaches a system wherein the stolen computer contains information, which may be secure, that identifies the computer. The information is sent by the computer over the network to a server module that has the “key” to identify the computer.

The Droz reference teaches, at the cited section, that the stolen computer can have a list of Domain Name System (DNS) information about the server modules to which the stolen computers can send the identifying information. Droz teaches not that the MAC information is hidden, but that the DNS information can be hidden in the stolen machine, such as in a hidden file or in a hard disk partition.

First, Droz does not teach the limitation of Applicant's invention "wherein the software...does not send physical addresses to the computer network". Droz teaches, at most, that its computer hides a list of addresses. Even the addresses that Droz hides are DNS addresses of remote server modules, not the MAC address of the stolen computer itself. Essentially, Droz teaches to hide the DNS list of server modules to which the stolen computer can report its identity.

Second, Droz teaches to send the MAC and other identifying information to the network. The computer system uses a network interface that typically comprises a transceiver that communicates with a medium access control (MAC) unit 12 (Droz, column 8, lines 63-66). The "computer system 40 announces its identity to the server module 42" (column 8, lines 14-16). "The secure identifier... is sent as so-called identity information across the network to the server module." (column 7, lines 2-4) "In the present embodiment the MAC unit 12 is used to send information to the network and receive information from the network" (column 9, lines 8-10).

Thus, the stolen computer does not hide its identity from the network. To the contrary, it announces its identity to a server module on the network. The Droz reference does not teach Applicant's claimed limitation of sending no physical address to the

network, but teaches away from Applicant's invention by teaching to send such information to the network. Despite the fact that the identifier is described as "secure", the identifying information is still being sent to the network, and could be obtained by a skilled hacker. Additionally, there is no teaching by Droz to hide the MAC address when this identifier is being sent. Indeed, because this is not described, it should be assumed that the MAC address is included in a conventional manner unless evidence is provided to the contrary. Droz presents no such evidence.

Thus, it would not have been obvious from Droz's teaching (to hide a list of network server addresses in a stolen computer that sends its identity over the network) to construct the claimed invention (that does not send a MAC address over the network). The teaching to hide information or send secure packets does not suggest to a person of ordinary skill to send no information about the physical address (MAC). The invention claimed is patentable over the prior art based at least on this distinction.

It should be noted in closing that the breadth of the claims is related to the groundbreaking nature and simplicity of the invention. A conventional computer network can be considered a set of network devices and "cables" (e.g., wires or wireless transceivers) for transmitting electrical signals (packets) between the network devices. Each cable of a network cable system is connected to each network interface of a network device to transmit the packets. Conventional network devices differ by network addresses, which are appointed to their network interfaces. Such network devices process and switch network packets (i.e., "traffic") between interfaces.

Special network devices, such as firewalls, protect the other network devices by filtration (acceptance or rejection) of network packets. In the claimed invention, one specific problem of protection is completely solved: susceptibility to hacking and other unauthorized access. This is accomplished by “full stealth” status, which means the invention is not just a screen that is difficult to hack into, but Applicant’s screen does not appear on the network as a visible device any more than a piece of cable.

This is accomplished by Applicant’s screen being different from a conventional network device, including conventional firewalls. Applicant’s “stealth” (hidden) status occurs due to the absence of sending any addresses that are appointed to the conventional firewall network interfaces. Applicant’s network screen seems effectively to be a part of the network cable system, not a network device.

It is well known that a pure cable does not participate in the processing of packets. Instead, a cable is used as the means for the transfer of packets. The cable environment is “transparent” or invisible to network protocols which use the network addresses. Therefore Applicant’s screen is a hidden feature of the network provided at a level of protocols which transmit network addresses. Of course, a firewall is visually distinguishable from a piece of a cable, but that fact does not require such a feature to be claimed. Therefore, the important identification attribute of network devices – sending physical addresses – is absent in the invention.

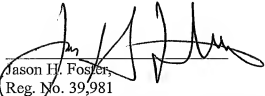
Therefore, the claims are allowable under 35 U.S.C. §102 and §103. Reconsideration and allowance are respectfully requested.

The examiner is authorized to communicate with the undersigned attorney by email by the following recommended authorization language: Recognizing that Internet communications are not secure, I hereby authorize the USPTO to communicate with me concerning any subject matter of this application by electronic mail. I understand that a copy of these communications will be made of record in the application file. (authorization pursuant to MPEP 502.03)

The Commissioner is authorized to charge Deposit Account No. 13-3393 for any insufficient fees under 37 CFR §§ 1.16 or 1.17, or credit any overpayment of fees.

Respectfully submitted,

07 May 2007
Date of Signature


Jason H. Foster,
Reg. No. 39,981
KREMBLAS, FOSTER, PHILLIPS & POLLOCK
7632 Slate Ridge Blvd.
Reynoldsburg, OH 43068
Voice: 614/575-2100
Fax: 614/575-2149
email: jfoster@ohiopatent.com